ORIGINAL

wrf

Wiley Rein & Fielding LLP **EX PARTE OR LATE FILED**

1776 K STREET NW
WASHINGTON, DC 20006
PHONE 202 719 7000
FAX 202 719 7049

Virginia Office
7925 JONES BRANCH DRIVE
SUITE 6200
McLEAN, VA 22102
PHONE 703 905 2800
FAX 703 905 2820

www wrf.com

October 15, 2003

RECEIVED

OCT 1 5 2003

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Robert L. Pettit
202.719.7019
rpettit@wrf.com

Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re. June 27, 2003 *ex parte* presentation in Savi Technology Request for Changes to Part 15 of the Commission's Rules; OET Docket No. 01-278.

Dear Ms Dortch:

On June 27, 2003, a letter was submitted on behalf of Savi Technology, Inc. ("Savi") in the above captioned proceeding. The letter was intended to: (1) apprise the Commission of an important new interference study conducted by the U.S. Navy, a study which demonstrates that the Savi system will not interfere with government radar systems; and (2) to request immediate action by the Commission to help implement the Homeland Security Act and the Marine Transportation Antiterrorism Act by granting the rule change proposed in the above-captioned rulemaking proceeding.

Savi hereby requests that the June 27, 2003 letter and all attachments be removed from the public record in the above captioned docket. In accordance with the Commission's rules, please include a copy of this letter and the attached revised version of the June 27, 2003 ex parte presentation with the record of this proceeding

If you have any questions or would like any additional information, please let me know.

Sincerely,

Robert L. Pettit
Counsel for Savi Technology, Inc.

Attachments

cc: Mr. Julius P Knapp, Deputy Chief, OET
Mr. Alan J. Scrime, Chief, Policy and Rules Division, OET
Ms. Karen E. Rackley, Technical Rules Branch Chief, Policy and Rules Division, OET

No. of Copies rec'd 0+1
List ABCDE

Stamp and Return

Wiley Rein & Fielding LLP

1776 K STREET NW
WASHINGTON, DC 20006
PHONE 202 719 7000
FAX 202.719.7049

Virginia Office
7925 JONES BRANCH DRIVE
SUITE 6200
McLEAN, VA 22102
PHONE 703 905 2800
FAX 703 905.2820

www.wrf.com

June 27, 2003

Robert L. Pettit
202.719.7019
rpettit@wrf.com

The Honorable Michael K. Powell
The Honorable Kathleen Q. Abernathy
The Honorable Michael Copps
The Honorable Kevin Martin
The Honorable Jonathan Adelstein
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, DC 20554

RE: *Ex parte* presentation in Savi Technology Request for Changes to Part 15 of the Commission's Rules; OET Docket No. 01-278

Dear Mr. Chairman and Commissioners:

On behalf of Savi Technology, which has been trying for more than two and a half years to secure a change in the Commission's Part 15 rules, this letter is intended: (1) to apprise the Commission of an important new interference study conducted by the U.S. Navy, a study which demonstrates that the Savi system will not interfere with government radar systems; and (2) to request immediate action by the Commission to help implement the Homeland Security Act and the Marine Transportation Antiterrorism Act by granting the rule change proposed in the above-captioned rulemaking proceeding.[1]

Savi is the maker of a radiofrequency identification (RFID) tag[2], which has been recognized to have obvious and immediate homeland security uses. Currently, the major customer for these tags is the United States Army.[3] At the Army's request,

---

[1] H.R. 5710, the Homeland Security Act, became Public Law 107-296 on November 25, 2002 and S. 1214, the Marine Transportation Antiterrorism Act, became Public Law 107-295 on November 25, 2002.

[2] The tag operates at 433.92 MHz and is compliant with Part 15 of the Commission's rules. Attachment A contains a brief explanation of the Savi system.

[3] As originally deployed, the tags were attached to military cargo containers so that military personnel could immediately locate and have access to military equipment. The tags were used extensively in the Bosnia campaign and, not surprisingly, have proved very popular with military operators. The tags can be read or loaded with data through a hard-wire connection (in locations where a computer database is readily available) or through a much more convenient and immediate wireless connection

Savi developed a new tag, capable of uploading and downloading tag information much more quickly than previous models.[4]

In addition to military use, the new RFID tag would also have a significant commercial application – one with a dramatic homeland security benefit – by providing an electronic manifest and seal for large ship-borne commercial cargo containers.[5] By using these devices, Customs agents, the U.S. Coast Guard or other security personnel could easily and immediately identify the contents of cargo containers and be able to tell whether tampering of the contents had occurred in transit to this country. Such a system would be invaluable for monitoring the millions of commercial cargo containers that enter the nation every year – a function that has grown even more critical in the wake of the September 11, 2001 terrorist attacks on the United States. Not surprisingly, the need for electronic sealing of cargo containers has been recognized in the last several months by the media[6] and Congress[7].

In fact, the function performed by these new devices is a precise goal of the antiterrorism legislation enacted by Congress and signed by the President. For example, S. 1214, the Maritime Transportation Antiterrorism Act, contains legislative findings that seaports, in particular, "are susceptible to large scale terrorism that could [threaten American citizens and] . . . could pose a significant threat to the ability of the United States to pursue its national security objectives."[8] The legislation further recognizes that "[c]urrent inspection levels of containerized cargo are insufficient to counter potential security risks" and that while "[t]echnology is currently not adequately deployed to allow for the non-intrusive inspection of containerized cargo," additional "promising technology is in the

---

[4] In essence, the Army wanted to increase the speed needed to upload and download up to 128 kilobytes of data stored on the RFID tag.

[5] Basically, the Savi RFID tags can be placed on commercial shipping containers, along with an electronic seal, to ensure that these containers are not tampered with during shipments and to ensure that security personnel can easily find out what is in the containers without having to open or X-ray them

[6] This gap in the nation's port security was highlighted in a *60 Minutes* broadcast more than a year ago A copy of this program has been submitted for the record in this proceeding.

[7] *See supra* note 1.

[8] Section 101(12), Page 4 of the Act.

process of being developed that could inspect cargo in a non-intrusive and timely fashion."[9]

Savi Request for Rulemaking. There is only one obstacle to the immediate implementation of this promising container security solution – an obstacle that the Commission has already proposed to remove. Operation of the new tag requires waiver or amendment of Part 15 of the Commission's rules to allow an increase in the so-called "duty cycle" for such RFID devices.[10] More than two and a half years ago, after consultation with the Commission and NTIA staff, Savi filed a petition for rulemaking to alter the duty cycle and has been attempting to secure this relatively small change to the rules ever since.[11] Importantly, Savi's request did not propose any increase in the amount of power that the devices are allowed to employ. It did not seek to change any other operational characteristic of the devices. Savi's request simply proposed that RFID devices be allowed to transmit for a longer time than is currently allowed under Part 15. That's all that would be needed to allow Savi's advanced RFID devices to operate.

Notice of Proposed Rulemaking. The Commission included Savi's request as part of a much larger Notice of Proposed Rulemaking.[12] Unfortunately (as events have transpired), the Commission altered Savi's original request in two significant ways that have drawn the concern of the National Telecommunications and Information Administration ("NTIA"): First, the Commission proposed to expand the allocation for RFID devices from two megahertz (433-435 MHz), as required by Savi, to ten megahertz (425-435 MHz). Second, while the Commission proposed no power increase for devices, like Savi's, operating at 433-435 MHz, it proposed a formula

---

[9] Section 101(8), Page 3 of the Act. The Homeland Security Act also creates an Undersecretary for Border and Transportation Policy charged with securing "borders, territorial waters, ports, terminals, and air, land, and sea transportation systems".

[10] "Duty cycle" refers to the amount of time a Part 15 device may transmit on a continuous basis. The current Commission requirements for device operations under Part 15 in the 433 MHz band limit transmissions on a continuous basis. For example, at the power levels Savi operates, the device can communicate for 10 seconds prior to shutting down for a period of time and then cycling on again for another 10-second transmission. If tags were required to operate in this on-off-on-off requirement, it would take up to 30 minutes to download the information from the Savi tag.

[11] *See* Savi Technology Petition for Rulemaking, filed November 22, 2000, RM-10051.

[12] *See Review of Part 15 and other Parts of the Commission's Rules*, ET Docket No. 01-278, *Notice of Proposed Rule Making and Order*, FCC 01-290 (October 15, 2001) ("*Part 15 NPRM*").

by which devices could operate at higher powers in other parts of the expanded band.[13]

NTIA Position. Savi attempted to coordinate with NTIA at various junctures in this process. In fact, during the past two years, Savi has had a series of meetings with NTIA staff, including a detailed technical briefing for the Interdepartment Radio Advisory Committee ("IRAC") more than a year-and-a-half ago. No formal or informal opposition to the Savi request was heard from IRAC, NTIA or any other government agency for more than a year after that briefing. However, on March 14, 2002, NTIA submitted a letter expressing its concern that the Commission's proposal would cause interference to government systems and promising a further analysis.[14] On October 15, 2002, the Acting Associate Administrator of NTIA filed a letter in this proceeding indicating that while NTIA "recognizes that RFID tags have the potential to be a publicly beneficial technology, particularly with respect to national security applications," NTIA could "not support" the proposals contained in the NPRM.[15] In essence, NTIA is concerned that systems operating pursuant to the Commission's proposal would cause harmful interference to certain government radar systems, in particular airborne radar systems.[16]

Savi Response. On October 28, 2002, Savi submitted a detailed technical response to the FCC staff. Savi will not repeat that analysis here – although appended to this letter is an attachment that refutes the major points raised by NTIA.[17] Suffice it to say that NTIA's position would significantly alter what has previously been considered "harmful" interference and simply ignores the real-world ability of government radar systems to process and ignore Part 15 emissions. Indeed, to adopt NTIA's view would be to admit that government radar systems are so fragile that

[13] *See Part 15 NPRM*; proposed new rule § 15.240.

[14] Letter from Fredrick R. Wentland, Acting Associate Administrator, Office of Spectrum Management, to Mr. Edmond J. Thomas, Chief, Office of Engineering and Technology (March 14, 2002).

[15] Letter from Fredrick R. Wentland, Acting Associate Administrator, Office of Spectrum Management, to Mr Edmond J. Thomas, Chief, Office of Engineering and Technology (October 15, 2002). This letter represented the first detailed explanation of NTIA's objections to the NPRM.

[16] As indicated above, the U.S. Army is Savi's primary customer for RFID devices and, in fact, suggested that Savi seek increased transmission authority in order to meet the Army's future needs. NTIA further urged the Commission to explore "other band options for this promising technology."

[17] See *Attachment B*

they could easily be defeated by Part 15 devices emitting 36 microwatts of power. Obviously – and happily for the security of the nation – this is not the case.

U.S. Navy Testing. Savi's interference analysis has essentially been confirmed by tests recently conducted by the U.S. Navy at Patuxent Naval Air Station. Due to the delays in receiving Commission approval of the proposed modifications to Part 15 and ongoing concerns expressed by DOD through NTIA, Savi agreed to and participated in a real-world interference test of its RFID tags conducted by the Navy. For this purpose, the Navy used its airborne radar, the APS-145 radar system. Significantly, the Navy's test report[18] concludes that radar operations were unaffected by the operation of the RFID system operating in either the normal mode or in the proposed 120 second mode of operation with radar signal processing (ECCM), turned on or turned off. Further, Savi's RFID operations were not completely degraded by the radar operations, even when in extremely close proximity. These test results are completely consistent with the technical analysis performed and provided to the Commission and NTIA almost a year ago and dramatically demonstrate that Savi's RFID tags will not cause harmful interference to DOD radar systems.

Further Savi Proposal. While Savi believes that NTIA's concerns, no matter how well intentioned, are unavailing, Savi recognizes that it is critical for this technology to be commercially deployed as soon as possible. Savi would be happy to operate under the proposal outlined in the Commission's NPRM. However, Savi would also be happy if the final rule were modified in ways that would not significantly harm the operational characteristics of Savi's RFID devices but would ameliorate NTIA's major concerns (and, in fact, more closely resemble Savi's original request). Accordingly, on October 15, 2002, Savi submitted a list of proposed modifications.[19] In particular:

- Savi currently operates only at 433.92 MHz. It has no desire to operate throughout the 425-435 MHz band and does not need to do so. Accordingly, Savi would support reducing the available band for advanced RFID products to 433-435 MHz. This more narrow allocation

[18] The Navy test report is included as Attachment C.

[19] Many of these modifications are more in line with what Savi had originally proposed to the Commission two years ago.

would be consistent with other international allocations and, at the same time, would eliminate NTIA's concerns about RFID operations throughout the entire 10 MHz band.

- As indicated above, Savi seeks no power increase for its products – merely an increase in the amount of time during which RFID devices can transmit – and believes that the FCC's proposal could be modified to clarify that no increases in power will be allowed in the band. In particular, Savi does not need a peak-to-average ratio of 20 dB, as proposed in the Commission NPRM, and could easily operate with a peak-to-average radio of 14 dB without adverse effect to its RFID products.

- NTIA is apparently concerned about the proliferation of products in this band, particularly if voice communications are allowed. Savi believes that the definition for RFID products could be strengthened to clarify that voice communications are not allowed in the advanced RFID band.

- NTIA is also apparently concerned about the possible geographic proliferation of devices in this band. Savi believes that the Commission could alter its proposal to limit use of devices in this area to commercial or industrial locations.

In addition to these steps (and in the interest of compromise), Savi believes that the proposed increase in duty cycle could be reduced from 120 seconds to 60 seconds without material degradation of the capabilities of Savi's RFID system.

As indicated above, Savi believes that these devices are critical to the security of the nation and critical to achieving the goals of the recently enacted antiterrorism legislation. Accordingly, Savi strongly encourages the Commission to move forward in permitting the modification to its rules to allow the enhanced use of RFID products for Federal and commercial purposes. As Savi has demonstrated clearly – and as has now been confirmed by the U.S. Navy – concerns that these products will cause harmful interference to government radar systems are inaccurate and are refuted by the characteristics of the bandwidth of each of these systems and the processing gains associated with the government radars.

By copy to the Commission's Secretary and in accordance with the Commission's rules, I request that this letter be filed with the record of the above-referenced rulemaking. Should you have any questions about this or if you would like any further information, please let me know.

Sincerely,

Robert L. Pettit
Counsel for Savi Technology, Inc.

Attachments

cc: The Honorable Nancy J. Victory
Fredrick R. Wentland
Marsha MacBride, Esquire
Mr. Edmund J. Thomas
Mr. Julius Knapp
Bryan Tramont, Esquire
Jennifer Manner, Esquire
Paul Margie, Esquire
Sam Feder, Esquire
Barry Ohlson, Esquire
Mr. Alan Scrime (FCC)
Mr. Ira Keltz (FCC)
Mr. Hugh Van Tuyl (FCC)
Geraldine Matisse, Esq.
Marlene Dortch (four copies for the record)

Attachment A: <u>Savi Technology and Container Security</u>

> "The stakes are high and the system is vulnerable, and we must do everything in our power to protect the global sea container trade, and we must do it now – before some devastating event occurs."
>
> *U.S. Customs Commissioner Robert C. Bonner*

Savi Technology currently produces RFID tags – operating on 433.92 MHz and compliant with Part 15 of the Commission's rules – used by the U.S. military to secure thousands of shipping containers of military equipment and material every day.

Recent breakthroughs in product design and technology have both increased the capability of these tags and reduced their cost to the point that they could immediately provide a cost-effective solution to shipping container and port security. The security vulnerability, as recently explained on *60 Minutes*, is obvious: more than 16 million shipping containers enter the United States every year. Until now, the only way to know what was inside them has been to physically inspect them, but U.S. Customs is able to *inspect only two per cent* of the containers entering the U.S. That means that there are *more than 15 and a half million uninspected cargo containers entering the country every year.*

Savi's new RFID tag is part of an electronic bolting system, called SmartSeal™. This system is used to seal and secure containers after they have been packed and inspected. Once secured, the SmartSeal™ tag can electronically detect and report any tampering activity, enabling continuous monitoring of the security status of the shipment. The system is virtually impossible to counterfeit or circumvent, and it uses encrypted communications protocols to ensure that its signals cannot be replicated. Thus, the system can tell U.S. Customs (or other security or port personnel): (1) where the container has been; (2) whether the container has been tampered with; and (3) the entire contents of the container.

Savi's new RFID tag has been recognized as a significant breakthrough in security technology. In fact, in the 2002 Supplemental Appropriations Act, the U.S. Senate notes the "proven technology and security standards" of the Savi system and encourages the Customs Service to "evaluate such best practices when investigating options for container security in ports it monitors." (S. 2551, p 91)

The information contained on the tag can be "read" in two different ways. First, it can be hardwired to a computer. However, as the U.S. Army has found, using a computer for this purpose is unwieldy and time consuming.

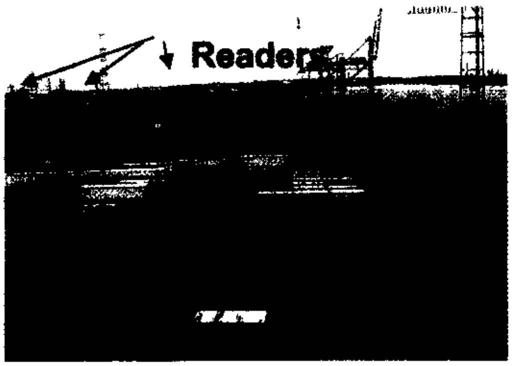
The information can also be "read" by using stationary or handheld wireless devices. These devices can be located throughout port facilities or carried by an inspector or other security or port personnel (See Figures 1-2.) and will allow the tags to be "read" quickly and conveniently as they are offloaded. If a container has been tampered with at any time during transportation, the system will issue an alert. The container can then be isolated and inspected or prevented from being loaded or moved.

Previous versions of the Savi RFID tag, which contained much more limited information, were able to operate within the current duty cycle rules of Part 15. Under current FCC rules, Savi's system can be "on" for no more than one second at a time – followed by a "silent period" between transmissions of at least 10 seconds.

However, because the new SmartSeal™ tags necessarily contain much more information, they require a longer time to "read" the information off the tag. In fact, under current duty cycle limitations, transmitting enhanced security information from a *single container* could *take up to 30 minutes.* Accordingly, providing for a longer "on" time is crucial for effective operation of the Savi RFID tag – and crucial to improving the transportation security of the United States.

Leveraging DoD Solution

Port of Antwerp



Implemented DoD Total Asset Visibility Network

- **World's largest active RFID network**
- **36 countries**
- **400 nodes worldwide – Airports, Seaports, Consolidation Points, and Railheads**
- **250,000 tracked conveyances and their items**
- **Open network, ISO and industry standards and protocols**
- **Combination of complementary technologies (active RF, GPS, barcode, data protocols)**
- **Available as global security infrastructure**

"Military Shipments are the most secure in the world - they have a sophisticated system that tracks everything they ship worldwide - we need a system with similar capabilities - but at a lower price point-for the millions of containers entering the US every year."

Rear Admiral Bennis DOT TSA

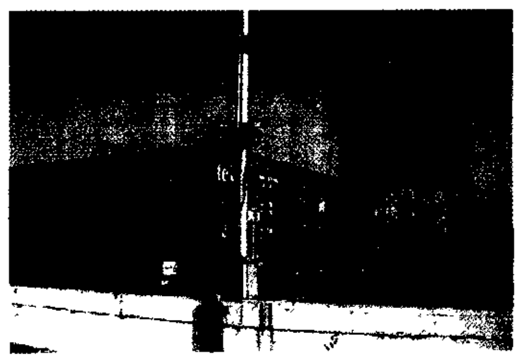


Figure 1

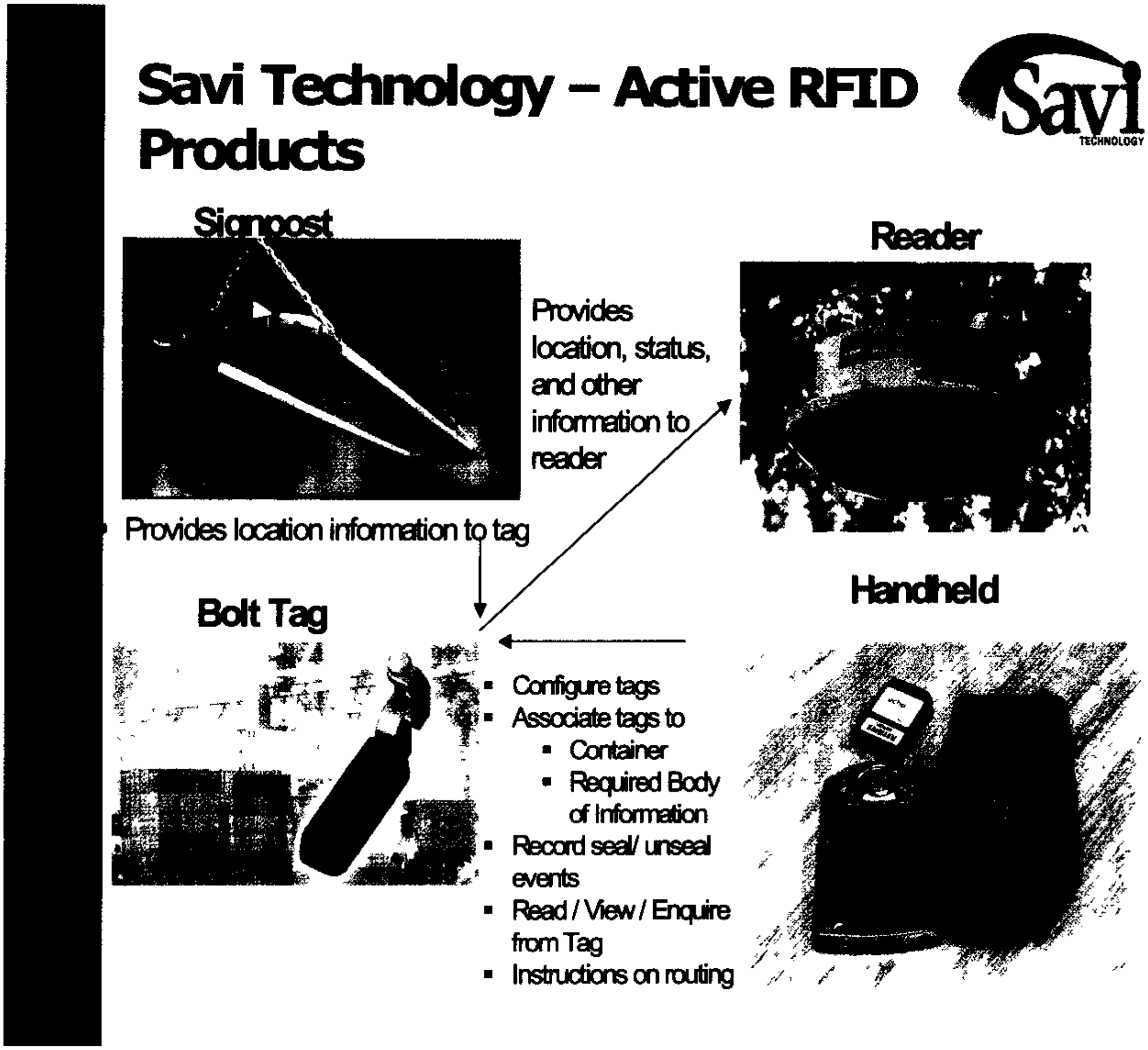

Savi Technology – Active RFID Products
Savi
TECHNOLOGY
Signpost
Reader
Provides location, status, and other information to reader
Provides location information to tag
Bolt Tag
Handheld
Configure tags
Associate tags to
Container
Required Body of Information
Record seal/ unseal events
Read / View / Enquire from Tag
Instructions on routing

Figure 2

Attachment B: Fundamental Deficiencies in NTIA Analysis

Fundamentally, NTIA's analysis (1) misperceives what Savi has requested and can operate with; and (2) does not recognize the ability of government radar systems to isolate and ignore emissions from Part 15 devices – just as they do today. If NTIA's analysis were correct, it would mean that government radar systems in the band already receive overwhelming interference both from RFID devices and amateur radio operators and that government radar systems are so fragile that they can be defeated by a few Part 15 devices operating at 3.6 milliwatts of power. NTIA's conclusions are not supported by the objective facts.[19]

♦ NTIA appears to misunderstand the need for a power increase. Savi needs no power increase to operate. The only change needed by Savi is an increase in "duty cycle" – i.e., the length of time Savi's devices are allowed to transmit. As is demonstrated in the NTIA analysis, the current average field strength limit is 11,000 microvolts per meter, and the current peak field strength limit is 110,000 microvolts per meter.[20] For systems using Savi's frequency band, 433-435 MHz, the exact same power limits would apply – before and after Savi's requested rule change.

♦ As a technical matter, under the existing rules, continuous transmissions are already possible, and already occur. The NTIA analysis fails to understand that the duty cycle is only a limit on a *single RFID interrogator communication with a single RFID tag*. The RFID interrogator is permitted to communicate with other tags during the "silent period" that it is not communicating with the initial tag. Thus, in particular deployments on military bases, Savi's interrogators are operating in a continuous fashion throughout the day, polling individual tags, one after the other. This operation is within the current NTIA and FCC rules and is permitted. What Savi seeks, and what does not cause additional harmful interference effects to Federal operations, is to permit these continuous

[19] A detailed review of NTIA's analysis was submitted to the record by Savi on October 15, 2002.

[20] *See* Table 1; Section 15 231(a)/(b) vs. Section 15.240 comparisons. Changes to Section 15.231(e) proposed by the Commission are not pertinent to the Savi system and are therefore not considered in this response.

ATTACHMENT C

transmissions to occur between a single tag and a single interrogator. Since Savi's rule change would only affect "duty cycle" and not power levels, it is obvious that if Savi's RFID devices were going to interfere with government radar, they would *already* be doing so.

- Thankfully for the sake of the nation's security, government radar systems are much more robust and sophisticated than is suggested by NTIA's analysis. Or to put it another way: Government radar systems really aren't so fragile that they can be defeated by extremely low-power Part 15 devices. NTIA does not make a distinction between harmful interference and the ability to "see" RFID devices. Savi's analysis shows that while radar facilities may be aware of RFID transmissions (and, of course, other transmissions, including amateur radio and numerous other Part 15 devices), this does not translate into harmful interference to government radar systems. In fact, government radar systems employ a variety of signal processing techniques used to isolate and reject amateur and Part 15 device transmissions. That's why amateur and RFID tags, which already operate in the band, don't harmfully interfere now. The NTIA analysis, if followed, would demonstrate that Amateur systems – operating at extraordinarily higher powers than RFID systems – are causing cataclysmic interference to government radar systems, a conclusion that flies in the face of actual operating experience. Clearly, this is not the case.

RFID/E-2C APS-145 UHF Radar
May 13, 2003 Test Results

Gene A. Robinson
Savi Technology

OVERVIEW

Since November 2000, Savi Technology has sought a slight modification to the duty cycle requirements for Part 15 radiofrequency identification (RFID) devices operating under Part 15 of the Commission's rules. In ET Docket No. 01-278, the FCC has proposed to modify its rules consistent with this request. However, NTIA and the Department of Defense (DOD) have expressed reservations concerning these rule changes. In response to these concerns, Savi Technology conducted an analysis, (Part 15 RFID Devices and DOD UHF Radar – Airborne, June 4, 2002) that indicated that its RFID FSK digital transmissions would not cause harmful interference to the radar operations that NTIA and DOD were attempting to protect. This analysis demonstrated that the RFID system would be detected by the APS-145 airborne UHF radar and eliminated with radar signal processing.

To provide qualitative and quantitative support of the written analysis performed by Savi Technology, a test was conducted May 13, 2003 at the Patuxent River NAS by the E-2C IPT using a Savi RFID interrogator, (Savi Reader 410R, Model SR-410R-016) operating with twenty RFID tags, (Savi Tag 412, Model ST-412-U1) and the E-2C APS-145 UHF airborne radar. This test had two main objectives: (1) to determine the effect of the E-2C UHF airborne radar on the RFID system while operating on the 433.92 MHz RFID operating frequency, and (2) to determine if the RFID system affected the operation of the E-2C APS-145 airborne radar system. The field test confirmed the previous written analysis as when the RFID signal was detected by the radar system, it was eliminated by the radar signal processing, ECCM.

The RFID system was detected by the APS-145 signal only while on the ground when positioned 500 feet from the test site. The RFID system was unaffected by the airborne radar signal when the aircraft was at ranges in excess of 100 Nm even though the C/I ratio at the RFID interrogator/reader was approximately –25 dB. At shorter ranges, (25 to 90 Nm), and worse C/I ratios, (-50 dB to –33 dB), the RFID system made use of the m/n retransmission algorithm to transmit the RFID tag information to the reader.

Test Overview

The test consisted of a ground reference test with the E-2C aircraft located approximately 500 feet from the RFID test site and an airborne test with altitudes up to 25,000 feet to maintain line-of-sight with the RFID system out to a distance of 195 Nm. The RFID system was operated at 433.92 MHz in both the normal mode of operation with tags transmitting for 1 second with a 10 percent duty cycle and a long mode of operation with tags transmitting for 120 seconds with a 10 percent duty cycle. The average power level of the RFID interrogator was 11,000 microvolts per meter as measured at 3 meters; (at the source the peak power was approximately -2.3 dBm, 0.58 milliwatts). The radar system operated in accordance with NATOPS for single medium PRF + 0.02 MW with the radar signal processing enabled and disabled. The radar antenna rotated at a rate of 6 rpm and the duration of main beam illumination of the RFID system was approximately 100 ms. The antenna sidelobe levels were 25 dB below the main beam peak.

The E-2C flight was initiated at the Patuxent River NAS designated as way point 1. The aircraft climbed to 25,000 feet on a 84 Nm outbound leg to the south to way point 2, and then to the east for 158 Nm. The aircraft then returned via this path back to Patuxent River NAS to complete the first part of the test. This route was flown a second time in a similar manner except prior to the outbound leg the aircraft delayed in the R-4006 area near the Patuxent River NAS and on the return leg between way point 2 and 1 the aircraft circled at the midpoint of that leg (40-50 Nm) and then descended for landing at Patuxent River NAS.

In the normal mode, the RFID interrogator would wakeup the tags and then have each of the tags transmit for 1 second, (ten 10-millisecond transmissions). This produced transmissions from the 20 tags every 10 milliseconds for 20 seconds followed by a 10-second quiet period. In the 120-second mode, the interrogator would wake up a tag and the tag would then send information for 120 seconds. The interrogator would then sequence to the next tag. This resulted in a continuous sequence of 20 millisecond transmissions every 100 milliseconds to support the test with the APS-145 UHF radar system.

The Savi RFID system uses a simple data parity check to detect errors. If an error occurs during a transmission a m/n algorithm is used to have retransmissions of the tag data. The system operator sets this parameter form one to a maximum of ten retransmissions based on the expected operating environment. The RFID system for this test was set for a moderate interference environment with a maximum of five retries. During the test, the retransmission algorithm was used by the RFID system the range to the E-2C aircraft was less than 90 Nm. At ranges of less than 25 Nm, the antenna sidelobe energy was sufficient to illuminate the RFID system on a continuos basis and resulted in the maximum use of retransmissions by the RFID tags. The RFID computer operating system provided visibility when retransmissions were occurring, the number of successful 10 millisecond data transmissions, the number of unsuccessful 10 millisecond data packets, and the percent of good data packets versus corrupted data packets. This test data is provided as an attachment to this report.

At the conclusion of the APS-145 UHF airborne test, an additional test was conduced by the E-2C IPT group using a broadband noise jammer located at the E-2C lab located approximately 4200 feet from the RFID system. The UHF noise jammer operated from levels of –15 dBm to +30 dBm. The +30 dBm noise level resulted in an interfering signal 25 dB greater than the desired RFID signal similar to the –25 dB C/I ratio obtained during the airborne radar test. Similar results were obtained in that the RFID system was able to operate with out any loss of transmissions and did not have to make use of the m/n retransmission algorithm for successful transmissions.

Data Analysis-RFID

The attached test data that shows the range of good data packets to the total data packets in percentage can be plotted as a function of the range to the E-2C aircraft. Then the nominal percent of successful data packet plot indicates the nominal performance of the system. The best and worse case performance can also be determined from the data extremes. This data is summarized below.

Range, Nm	Percent Good Packets to Total Best	Nominal	Worse	Desired to Interference Ratio, C/I in dB
170	100	100	100	-15
150	100	100	90	-19
125	100	90	75	-24
100	95	78	65	-30
90	90	75	58	-32
75	80	65	50	-36
50	62	52	37	-40
25	45	40	25	-45

As can be seen from the above, the RFID data packets begin to be affected with C/I ratios of –19 dB to –30 dB and at distances to the aircraft of 100 Nm to 150 Nm. During this time, it was observed that the data was successfully retransmitted with one additional retransmission. As the interference increased, the number of data packets affected increased as expected but the m/n algorithm with retransmission set at 5 allowed successful transmission of the data packet under the worse case conditions experienced.

The airborne test results reported in the attached report indicates that the RFID system performance was at least 95% (ratio of good data packets to total packets) where the radar radiated power translated to a level of –30 dBm and degraded to approximately 30% at –24 to –21 dBm levels. The retransmission algorithm was effective in allowing successful transmission of the data from the tag to the reader.

The RFID system data taken during the broadband noise interference noise test also indicated 100 percent data packet transmissions between the RFID tags and interrogator/reader with negative C/I ratios of –25 dB.

Data Analysis-Radar, APS-145

The E-2C APS-145 radar test report, "RADIO FREQUENCY IDENTIFICATION (RFID) TAGS INTEREFERRENCE TEST FLIGHT REPORT", is attached. The RFID normal and 120-second operating modes produced a series of small radial dots, "rabbit tracks", (normally referred to as fruiting), on the radar PPI scope at a range distance of approximately 500 feet from the test site. In addition, a 10 Nm degradation in multi-rings was seen with the RFID system operating in the 120-second mode and the radar ECCM mode turned off. Radar signal processing, (ECCM mode, the normal radar operating mode), eliminated all tracks from the RFID system. During the APS-145 radar ground test, a 3% fluctuation in channel quality was observed with the ECCM while the RFID system was operating and also when the RFID system was turned off. It was assessed as very likely that the fluctuation was due to a source external to the test.

The APS-145 radar experienced no operational effects while airborne in the area or throughout the flight test with the RFID either operating in it's various modes or turned off. The heavy air traffic areas of Baltimore and Washington were 30 degrees off axis from the Patuxent River NAS test site and traffic in those areas were easily distinguished and separated.

Summary

The APS-145 radar system normal operation was found to be unaffected by the operation of the RFID system operating in either the normal mode or in the proposed 120 second mode of operation with radar signal processing, (ECCM), turned on or turned off. While on the ground, 500 feet from the test site minimal affects were noted with ECCM turned off but with ECCM on absolutely no effects were seen.

The Savi RFID system was unaffected by the APS-145 radar signal with up to –25 dB desired signal to interference signal ratios, (radar signal 25 dB higher than the RFID signal). At larger interference levels, (-33 to –50 dB), the RFID retransmission algorithm allowed the reader/interrogator to continue successful data exchanges with the tags in both the normal and 120-second mode of operation.

The RFID and E-2C APS-145 UHF Radar test was successful in that all test objectives were met, the APS-145 operational capability was not affected by the RFID system, the RFID system continued to operate successfully and the previous analysis of coexistence was verified.

Attachments

1. RFID Test Data, May 13, 2003.
2. Radio Frequency Identification (RFID) Tags Interference Flight Report, June 3, 2003, Naval Air Warfare Center Aircraft Division Patuxent River, Maryland.

Attachment 1

Savi Technology RFID
And
E-2C UHF Radar Test Data

Date: May 13, 2003
Location: Patuxent River NAS
Aircraft: E-2C A/C No. 849
Test Scenario:

Ground reference data, preflight: Taxi aircraft to RW 14 intersection B (500-1000 feet from RFID system test site), for radar receiver reference data using a spectrum analyzer connected to the UHF radar diplexer and the radar receiver with the antenna diplexer connected to radar system.

Flight data: Take off and perform a maximum climb with the APS-145 UHF radar operating from WP1, (Patuxent River NAS) to 25,000 feet on the outbound leg to WP2, then fly east to WP3 for maximum range of 195 Nm. Fly west back to WP2 and turn north toward WP1. On the inbound leg at approximately the half way point, (40 to 50 Nm range) circle twice before starting the decent from 25,000 feet on the way back to WP1, (Patuxent River NAS). Check the multi-ring range, PPV lobe, channel quality and range to target with the ECCM processing turned on and off.

WP1(dms):	N 38 17 14	W 076 24 12
WP2(dms):	N 36 55 00	W 072 42 00
WP3(dms):	N 35 55 00	W 072 42 00

RFID System: Operate the RFID interrogator/reader and tags in both the normal mode of operation and in the 120-second data mode. While the E-2C aircraft is outbound and inbound monitor and record the quality of the communication link between the RFID interrogator and tags. Observe and record the aircraft reported range, spectrum analyzer signal levels and the number of pass/fail transmissions.

Post Flight Test – Noise Test: Following the flight test observe the operation on the RFID system in the presence of a broadband noise jammer operated from the E-2C Lab approximately 4200 feet from the RFID system test area. Monitor and record the quality of the communication link between the RFID interrogator and tags during the times the noise jammer is transmitting at –15 dBm, -10 dBm and +30 dBm.

RFID Test Data
May 13, 2003

Time	Event/Mode/Range	Status:Pass/Fail , %Pass, Comments
10:00 AM	Preflight Test Check, Radar not Transmitting.	Normal mode, 100% first 3 cycles, 30x10 on all 20 tags. Then on cycle 4 lost all tags except for 364,365,and 368.
10:10 AM	Preflight Test Check, Radar not Transmitting.	Changed to second interrogator/reader and received reader error message. Switched back to first reader.
10:15 AM	A/C positioned at taxiway intersection B to RW14 approximately 500' from test sight. Tags in Normal Mode: 1 sec. transmit of ten 10ms data packets. Radar not Transmitting.	Pass/Fail ranging in 88/2,92/8,99/1,90/10 for ten cycles, (100 data packets) for each of the 20 tags. Some indication of AC Generator problems.
10:20 AM	Tags placed in 120-second mode. Radar not Transmitting.	RFID level at the E-2C antenna diplexer is –55 dBm.
10:26 AM	Interrogator/Tags Off. Radar not Transmitting.	Radar reference with out the RFID system operating.
10:36 AM	Tags placed in 120-second mode. Radar not Transmitting.	Tag 428364; 964/11, 98% Note: F18 passed during 11 failed tries. Tag 428365; 508/21, 98%, 660/23, 97%, 718/39, 95%, 936/39, 96%. Tag 428366; 75/5,95%, 218/10, 96%.
10:42 AM	Tags in Normal Mode.	75 to 100% passed.
10:50 AM	Tags in 120-second mode.	127/30, 138/50, 300/55, 669/72, 800/72, 889/86, 100/0, 300/0, 335/9, 820/18.
11:00 AM	RFID system turned off.	
11:02 AM	RFID system turned on in 120-second mode. Radar not Transmitting.	Tags ranging from 89% to 99% successful data transmissions.
11:13 AM	RFID system turned off.	A/C taxied to takeoff position.
11:14 AM	UPS put on line to clean up generator power.	UPS failing and 50 % of transmissions in the RFID system failing.
11:33 AM	Aircraft radar on and Tags in Normal Mode.	Approximately 50% of RFID transmissions failing. M/N algorithms (set to 5 retries) working to successfully pass data from tags.
11:36 AM	UPS removed from system.	RFID system restarted in 120 second transmit mode. 40/0, 100%

RFID Test Data
May 13, 2003

Time	Event/Mode/Range	Status:Pass/Fail , %Pass, Comments
11:37 AM	System Restarted	UPS out of line.
11:33 AM	A/C 165 Nm outbound, 25000 feet. Normal mode.	40/0, 100 % Contact with aircraft lost.
12:36 AM	A/C 151 Nm inbound. Tags in 120-second mode.	Tags performance about same as with radar off, 80-90% pass.
12:36 AM+	A/C 141 Nm. Tags in 120-second mode.	Tag 4283664 457/57, 88%
12:41 AM	A/C 131 Nm. Tags in 120-second mode. Main beam approximately 100 ms.	897/78, 92%; 499/45, 92%; 744/87, 89%; 870/105, 89%; 770/205, 78%
12:50 AM	A/C 94 Nm. Tags in 120-second mode.	428367-428368; 696/170, 80%; 708/204, 77%; 750/225, 76%; 83/16, 85%.
12:58 AM	A/C 83 Nm.	285/49, 85%, 684/140, 82%
1:00 PM	A/C <80 Nm	799/170, 82%
1:04 PM	A/C 40 Nm	34/24, 61%; 147/102, 58%; 250/200, 55%; 298/249, 54%; 390/326, 55%; 411/345, 54%, 439/400, 52%; 511/456, 53%
1:09 PM	A/C 49 Nm	4283670, 12/26, 35%; 34/55, 40%, 4283670, 60/122, 32%; 77/172, 30%; 99/229, 30%. A/C radar signal level is –18 dBm peak.
1:11 PM	A/C 27 Nm	117/254, 31%; 152/328, 31%; 173/425, 28%; 191/522, 26%
1:16 PM	Radar Signal –12 dBm	216/633, 25%; 235/728, 24%
1:18 PM	Tags still in 120-second mode. Radar – 20 dBm.	428371, 19/19, 50%; 50/88, 35%; 77/197, 28%; 96/231, 29%; 115/253, 31%; 150/304, 33%; 201/335, 37%.
1:22 PM 1:25 PM	A/C range 18 Nm. and signal at –18 dBm.	223/419, 35%; 316/547, 37%; 379/574, 40%, 395/580, 40%.
1:26 PM	Radar signal –20 dBm to –30 dBm.	428372, 12/27, 38%; 54/65, 47%; 99/118, 46%; 234/202, 53%; 305/293, 51%; 362/344, 51%.
1:37 PM	A/C range 68 Nm. Radar signal –30 dBm.	428373, 114/85, 58%; 203/125, 62%; 248/138, 65%; 694/281, 71%; 694/281, 71%; 694/281, 71%.

RFID Test Data
May 13, 2003

Time	Event/Mode/Range	Status:Pass/Fail , %Pass, Comments
1:43 PM	A/C range 94 Nm. Radar signal level –32 dBm. Range 105 Nm, -33 dBm.	428374, 778/78, 90 %, 889/86, 91%; 428375, 115/8, 94%; 260/12, 95%; 533/124, 80%; 533/176, 79%; 533/384, 58%; 533/442, 54%.
1:56 PM	A/C range 114 Nm. A/C range 127 Nm, Signal level -35 dBm.	428376, 127/2, 98%. 127/2, 98%.
1:56 PM	Computer rebooted.	
1:56 PM	Radar signal –42 dBm	428364, 145/15, 93%; 450/48, 90%; 500/49, 91%; 618/52, 93%; 885/53, 94%.
1:59 PM	A/C range 160 NM, Radar signal –49 dBm.	428365, 96/0, 100%, 147/0, 100%; 260/1, 99%; 480/1, 99%; 972/3, 99%.
2:03 PM	Radar signal –50 dBm. Radar signal –51 dBm.	428366, 610/4, 99%. 870/5, 99%.
	Tag signal level –64 dBm. Noise Floor –75 dBm. Radar Signal –49 dBm.	428637, 280/0, 100%; 400/0, 100%; 500/0, 100%; 770/0, 100%. 428638, 662/0, 100%; 428369, 974/1, 99%
	Radar Signal –45 dBm.	428370, 120/3, 89%; 175/22,89%; 355/26, 93%, 472/26,94%; 760/37, 95%.
	Radar Signal –46 dBm.	428371, 220/0, 100%; 385/0, 100%; 500/0, 100%; 600/1, 99%; 750/2, 99%; 900/2, 99%, 973/2, 99%.
2:19 PM	A/C range 159 Nm., signal level -48 dBm	428372, 200/0, 100%; 325/0, 100%; 425/0, 100%; 615/0, 100%; 700/0, 100%; 880/0, 100%; 975;0, 100%.
		428373, 100/1, 995; 225/1, 99%; 350/1, 99%; 500/3, 99%; 635/4, 99%; 775/5, 99%; 900/6, 99%; 935/40, 95%.
2:28 PM	A/C range 129 Nm. Signal level –35 dBm, range 118 Nm	428374, 0/50, 0%; 0/100, 0%; 0/200, 0%; 0/453, 0%; 0/520, 0%; 0/975, 0%.
2:34 PM	Change Battery in tag 428374	
2:36 PM	Signal level –29 dBm. A/C range 107 Nm, signal level –32 dBm.	428375, 148/6, 96%; 265/10, 96%; 345/11, 96%; 469/16, 96%.

RFID Test Data
May 13, 2003

Time	Event/Mode/Range	Status:Pass/Fail , %Pass, Comments
3:00 PM	NOISE TEST	Noise Jammer located at the E-2C lab with levels of –15 dBm to +30 dBm were used to evaluate the RFID system. The lab location was 4200 feet from the RFID setup.
	RFID System on line. Noise source output level of –15 dBm.	Spectrum analyzer at the RFID location measured –69 dBm. Tag 428367 transmitted 120 seconds with no drop out of data or use of m/n error detection algorithm. 45/0, 100%; 132/0, 100%; 316/0, 100%; 375/0, 100%; 674/0, 100%; 975/0, 100%
	Noise source output level of –10 dBm.	Tag 428368 transmitted with no drop out of data or use of error detection algorithm for retransmission. 221`/0, 100%.
	Noise source output level of +30 dBm.	Spectrum analyzer at the RFID location measured –47 to –40 dBm. Tag 428368 transmitted with no drop out of data. 558/0, 100%.
3:08 PM	NOISE TEST ENDED	
	RFID System off-line.	

RFID Test Data
May 13, 2003

Time	Event/Mode/Range	Status:Pass/Fail , %Pass, Comments
	Reboot computer and switch tags to Normal mode.	
	A/C signal level –29 dBm A/C range 88 Nm.	First cycle: Tag 428366 10/1, 90% Tag 428369, 10/1, 90% Tag 428370, 10/2, 80% Tag 428364/65/68, 10/10, 100%, Other tags: 5/5, 50%.
2:42 PM	Switch tags to 120-second mode.	
  2:45 PM	A/C range 88 Nm, radar signal –46 dBm. Radar signal –44 dBm. Radar signal –30 dBm.	428364, 90/32, 74%; 180/79, 68%; 195/98, 66%; 208/113, 69%; 270/160, 62%; 321/215, 60%;
2:46 PM	Radar range 70 Nm, radar signal –29 dBm. Radar signal –34 dBm. Radar signal –28 dBm.	392/2276, 58%; 429/316, 57% 458/376, 54% 483/413, 53%; 513/462, 52%.
2:50 PM	Radar signal –24 dBm Radar range 58 NM	428365, 4/53, 6%; 9/72, 17%. Tags signal 2 dB greater than radar sidelobes. Tags under continual illumination. 43/137, 24%;87/195, 31%; 119/237, 32%;
2:53 PM	A/C range 46 Nm., signal level –21 dBm.	138/517, 30 %. Tag signals not visible on spectrum analyzer due to radar signal level.
2:55 PM	A/C inbound, 13,000 feet. Radar signal –20 dBm. Radar signal –16 dBm. Radar signal –15 dBm A/C range 34 Nm., -15 to –18 dBm.	428365, 132/427, 27%. 165/456, 26%. 184/500,26%; 193/542, 26%. 204/604, 25%; 239/683, 26%.
	Sidelobe levels –17 dBm, continuos illuminations, main beam off-scale.	428366, 1/16, 8%; 5/58, 8%; 100/181, 40%; 335/197, 57%, 728/197, 79%
3:00 PM	RFID system off-line	